200Mbps Powerline
PLV-200AV-PEWN

User Manual
V1.0

Contents

1 Overview 1
2 Hardware Description 3
2.1 LED Status and Button Description 3
2.2 Interface Description 5
2.3 Hardware Installation 6
2.3.1 System Requirements 6
2.3.2 Before You Begin 6
2.4 Operation Range 6
2.5 How to Improve the Transmission Capacity 6
3 Wireless Network Configuration 8
3.1 TCP/IP Settings 8
3.2 Log In to the Web Page 11
4 Web Configuration 12
4.1 Status 12
4.1.1 Device Information 12
4.1.2 Network Information 12
4.1.3 User Information 13
4.2 Network 15
4.2.1 Network Settings 15
4.2.2 LAN Settings 18
4.2.3 WLAN Settings 20
4.2.3.1 Radio settings 22
4.2.3.2 Wireless Settings 23
4.2.3.3 Wireless Security Mode 24
4.2.4 Time Management 29
4.2.5 Router Settings 30
4.2.5.1 Dynamic Route 31
4.2.5.2 Static Route 32
4.2.6 Powerline Settings 33
4.2.6.1 Local Device Configure 35
4.2.6.2 Remote Device Configure 35
4.2.6.3 Advance Configuration 36
4.3 Security 36

4.3.1 WAN Access Configuration 37
4.3.2 Firewall 38
4.3.3 MAC Filter 39
4.3.4 Port Filter 39
4.4 Application 41
4.4.1 DDNS Configuration 41
4.4.2 Advanced NAT Configuration 42
4.4.3 UPnP Configuration 46
4.4.4 IGMP Settings 46
4.4.5 Microsoft LLTD Settings 47
4.5 Management 47
4.5.1 Device Management 47
4.5.2 User Management 48
4.5.3 Log File Management 49
5 How to Use the Security Pushbutton 50
5.1 Forming a HomePlug AV logical network 51
5.2 Joining a Network 51
5.3 Leaving a Network 52
6 Parameter and Specification 54

About User Manual

This user manual mainly describes how to install and configure the PLV-200AV-PEWN wireless extender.

Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1 : Overview	Provides a general overview of the PLV-200AV-PEWN wireless router, and the package list.
Chapter 2 : Hardware Description	Describes the front panel and the rear panel of the PLV-200AV-PEWN and the procedure for hardware installation.
Chapter 3 :Wireless Network Configuration	Describes how to configure network settings of your PC, and then connect to the PLV-200AV-PEWN.
Chapter 4 : Web Configuration	Describes how to navigate through the Web pages and how to configure the parameters.
Chapter 5 : How to Use the Security Pushbutton	Describes how to use the Security Pushbutton
Chapter 6 : Parameter and Specification	Introduce the product system specification

Features

PowerLine Feature

- Power supply range of 100 ~ 240VAC 50/60Hz
- Comply with HomePlug AV, and Co-existence with HomePlug 1.0 Nodes
- PowerLine PHY rate up to 200 Mbps

- Support QAM 1024/256/64/16/8, QPSK, BPSK, and ROBO modulation schemes
- 128-bit AES Link Encryption with key management for secure power line communications
- Windowed OFDM with noise mitigation based on patented line synchronization techniques improves data integrity in noisy conditions
- Dynamic channel adaptation and channel estimation maximizes throughput in harsh channel conditions
- Priority-based CSMA/CA channel access schemes maximize efficiency and throughput
- Integrated Quality of Service (QoS) Enhancements: contention-free access, four-level priority based contention access, and multi segment bursting
- ToS and CoS Packet Classifiers
- Supports IGMP managed multicast sessions

Wireless Feature

- Support IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i, and IEEE802.11e
- Support 1T1R mode and transmission data rate is up to 150 Mbps
- Support WEP and WPA for data transmission security
- Support DHCP Server and Client
- Support firmware version upgrade via Web page
- Support restoring factory default settings
- Support wireless security authentication modes, including OPEN, WEP, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK, 802.1X, WPA/WPA2-Enterprise.
- Support system status display
- Support system log

1 Overview

Thank you for choosing PLV-200AV-PEWN.

PLV-200AV-PEWN (also called PLC Wireless Extender) is compatible with HomePlugAV, HomePlug 1.0, and 802.11b/g/n standards. PLV-200AV-PEWN supports CCK and OFDM. Its PowerLine PHY rate is up to 200 Mbps and wireless PHY rate up to 150 Mbps under the 11n mode.

PLV-200AV-PEWN supports 128-bit AES encryption in PowerLine communication, and WEP, WPA, and IEEE 802.1X authentication in wireless communication, to ensure wireless communication security.

Package list

Please check whether your package list includes the following items:

- PLV-200AV-PEWN x 1
- CD-ROM x 1
- RJ45 x 1

Security Notes

PLV-200AV-PEWN is intended for connection to the AC power line. For installation instructions, please refer to the installation section of this user manual. Before operating PLV-200AV-PEWN, read the following precaution information carefully:

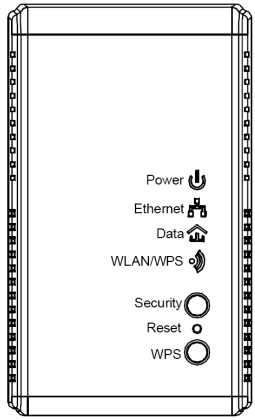
- Follow all warnings and instructions marked on the product.
- Unplug the device from the wall outlet before cleaning. Use a damp cloth to clean the device. Do not use liquid cleaners or aerosol cleaners.
- Keep the device away from water.
- Keep the device away from radiators or heat registers.
- Do not use an extension cord to connect the device and the AC power source.
- Do not open the device to perform maintenance on your own. Otherwise, you may get an electric shock. Ask professional technicians to maintain the device.
- Unplug the device from the wall outlet and contact professional service personnel for help if you encounter the following situations:
  - Liquid is spilled into the device.
  - The device is exposed to rain or water.

- The device fails to operate normally when you follow the operation instructions to operate it.
- The performance of the device changes obviously.

2 Hardware Description

2.1 LED Status and Button Description

There are 4 LED indicators on the front panel of PLV-200AV-PEWN. By observing their status, you can judge whether the device runs normally.



The following table describes the LED status on the front panel.

LED Indicator	Color	Status	Description
Power	Green	On	The device is powered on.
	Green	Blink	● System enters the power save mode. ● System is resetting. ● System is in the process of security setup.
	-	Off	The device is powered off or it is down.
Ethernet	Green	On	LAN connection succeeds.
	Green	Blink	Data is being transmitted in the LAN.
	Red	On	WAN connection succeeds.
	Red	Blink	Data is being transmitted in the WAN.
	-	Off	No LAN or WAN connection
Data	Green	On/Blink	PLC rate > 40 Mbps

LED Indicator	Color	Status	Description
	Orange	On/Blink	20 Mbps < PLC rate < 40 Mbps
	Red	On/Blink	PLC rate < 20 Mbps
WLAN/WPS	Green	On	The WLAN connection has been activated.
	Green	Blink	Data is being transmitted in the WLAN.
	-	Off	The WLAN connection is not activated.
	Red	On	Connection succeeds under Wi-Fi Protected Setup.
	Red	Blink	Negotiation is in progress under Wi-Fi Protected Setup.
	-	Off	Wi-Fi Protected Setup is disabled.

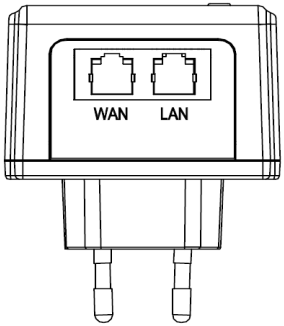
The following table describes the buttons on the front panel.

Button	Description
Security	The **Security** button is used to set the membership status. ● Pressing and holding the **Security** button for more than 10 seconds randomizes the NMK value. ● Pressing and holding the **Security** button for 0.5 to 3 seconds makes the adapter a member of the existing AVLN.
Reset	Use a fine needle to press **Reset** gently for 4 seconds and then release the button. The system reboots and restores to the factory defaults.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the extender starts to accept the negotiation of PBC mode.

🕮 **Note:**

Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 4 seconds with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

2.2 Interface Description



The following table describes interfaces and buttons on the rear panel.

Interface/Button	Description
WAN	RJ45 WAN interface, for connecting WAN or the uplink network devices.
LAN	RJ45 LAN interfaces, for connecting hub, switch, or computer in an LAN.

2.3 Hardware Installation

2.3.1 System Requirements

Before installing PLV-200AV-PEWN, please make sure that the following items are available.

- At least one Ethernet RJ45 cable (10Base-T/100Base-T)
- One PLV-200AV-PEWN
- One PLC device for PowerLine communication
- A PC is already installed with the TCP/IP protocol and it can access the Internet.

2.3.2 Before You Begin

Before you install PLV-200AV-PEWN, please pay attention to the following items:

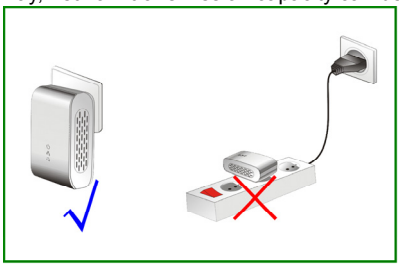
- The Ethernet cables that are used to connect to a computer, hub, router or switch should be less than 100 meters.
- Do not place this device on an uneven or unstable surface or support. Do not put this device on the ground.
- Keep the device clean. Prevent the device from direct sunlight. Avoid any metal in the device.
- Place the device in the center of the area, and try to optimize the wireless coverage.

2.4 Operation Range

The operation range of PLV-200AV-PEWN depends on the actual environment. The path and effect of signal transmission vary with the deployment in a house or an office. For PLC networks, the typical coverage is up to 5000 square feet, but the actual coverage varies with the power grid and the number of connected PLC terminal devices. For wireless transmission, the outdoor straight transmission distance for some devices can reach up to 300 meters, and the indoor straight transmission distance can reach up to 100 meters.

2.5 How to Improve the Transmission Capacity

It is recommended to plug PLV-200AV-PEWN directly into a wall socket, not to a power strip. In this way, network transmission capacity can be optimized.



3 Wireless Network Configuration

The Web management tool allows you to configure wireless function of PLV-200AV-PEWN and PLC function, the recommended browser is IE 5.0 or above.

The following sections describe how to set the Internet connection, local Ethernet connection, and wireless connection, and how to access the Web page of PLV-200AV-PEWN.

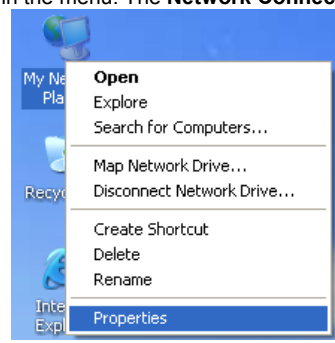
3.1 TCP/IP Settings

By default, the LAN IP address of PLV-200AV-PEWN is 192.168.0.1, the subnet mask is 255.255.255.0, and the DHCP server is enabled.

It is recommended you set the network adapter to be **Obtain an IP address automatically**. Your PC acquires IP address, subnet mask, gateway, and DNS address automatically via the extender. If you know the setting of the current LAN interface, you can manually set the TCP/IP properties of the network adapter, so that your PC can communicate with the extender.

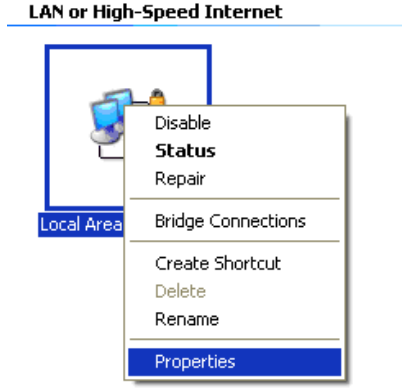
You may manually set the network adapter by following the steps below:

Step 1 Right click the icon of **My Network Places** (e.g., Windows XP) and select **Properties** in the menu. The **Network Connections** page appears.

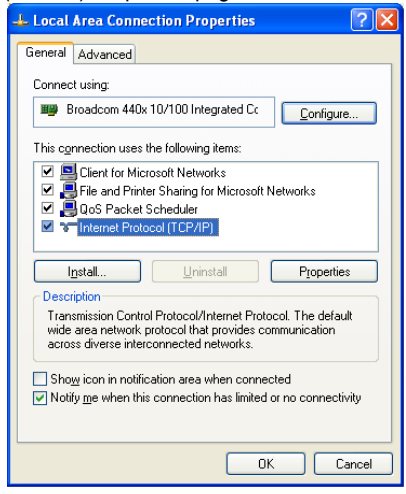


Step 2 Right click the network adapter icon and select **Properties** in the menu. The **Local Area Connections Properties** appears. (**Note:** If there are

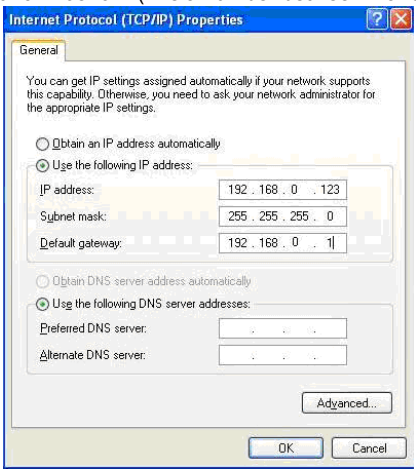
several network cards on your PC, it may not display the **Local Area Connections Properties** page. It may display other dialog boxes.)



Step 3 Double click the Internet Protocol (TCP/IP) to display the Internet Protocol (TCP/IP) Properties page.

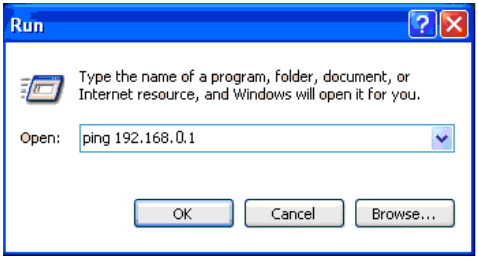


Step 4 Select **Use the following IP address** and enter the IP address of the network adapter. The IP address should belong to the IP network segment 192.168. 0.X (X is a number between 2 and 254).


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 123
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Step 5 Set the subnet mask and then click the **OK** button to finish manual setting.

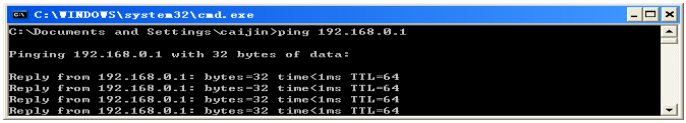
Step 6 After finishing setting, you may ping the default IP address of the extender, to check whether the current connection between PC and the extender is normal. Click **RUN…** in the lower left corner on the desktop, and then enter **ping 192.168.0.1** in the dialog box. See the following figure:



Note:

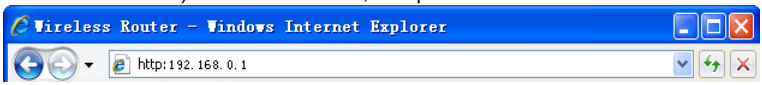
192.168.0.1 is the default IP address of the LAN interface. If this IP address is changed and you need to ping the IP address of the extender, you should enter the current IP address in the dialog box above.

Step 7 If PC can ping through the default IP address of the extender and the following page appears, it indicates that the connection between PC and AP is normal.

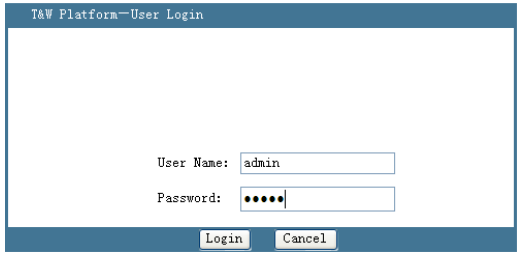

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\caijin>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

3.2 Log In to the Web Page

Run the Internet Explorer (IE), enter ***http://192.168.0.1/*** (the default IP address of PLV-200AV-PEWN) in the address bar, and press **Enter**.



Enter the user name (***admin***, by default) and the password (***Password***, by default) on the login page.



After clicking the **Login** button on the login page, you can log in to the Web page of the PLV-200AV-PEWN.

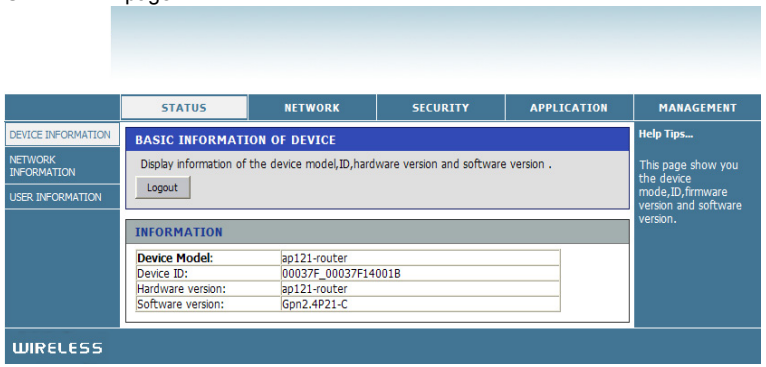
4 Web Configuration

4.1 Status

After logging in to the Web page, system automatically displays the **STATUS** page. The submenu of **STATUS** contains **DEVICE INFORMATION**, **NETWORK INFORMATION**, and **USER INFORMATION**.

4.1.1 Device Information

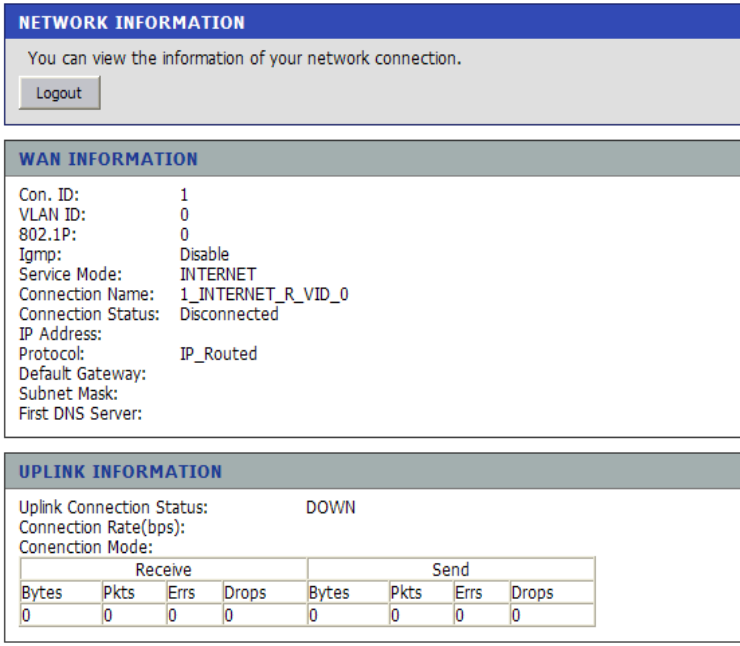
Choose **STATUS** > **DEVICE INFORMATION** to display the **BASIC INFORMATION OF DEVICE** page.



In this page, you can view the device model, the ID, the hardware version, and the software version.

4.1.2 Network Information

Choose **STATUS** > **NETWORK INFORMATION** to display the **NETWORK INFORMATION** page.



NETWORK INFORMATION

You can view the information of your network connection.

Logout

WAN INFORMATION

Con. ID:	1
VLAN ID:	0
802.1P:	0
Igmp:	Disable
Service Mode:	INTERNET
Connection Name:	1_INTERNET_R_VID_0
Connection Status:	Disconnected
IP Address:	
Protocol:	IP_Routed
Default Gateway:	
Subnet Mask:	
First DNS Server:	

UPLINK INFORMATION

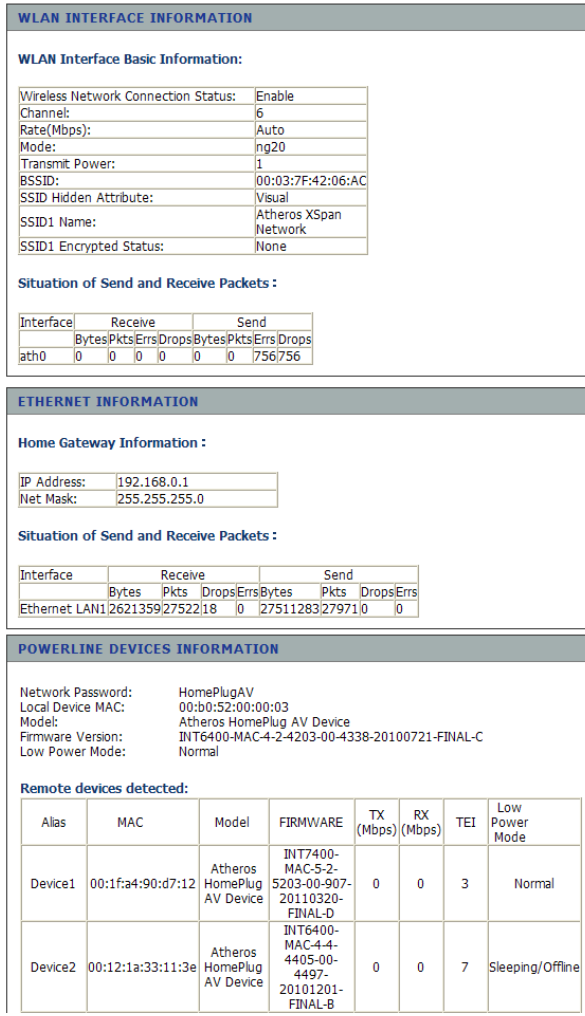
Uplink Connection Status: DOWN
Connection Rate(bps):
Conenction Mode:

Receive				Send			
Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
0	0	0	0	0	0	0	0

In this page, you can view WAN and uplink information of the device.

4.1.3 User Information

Choose **STATUS** > **USER INFORMATION** to display the **USER INFORMATION** page.



WLAN INTERFACE INFORMATION

WLAN Interface Basic Information:

Wireless Network Connection Status:	Enable
Channel:	6
Rate(Mbps):	Auto
Mode:	ng20
Transmit Power:	1
BSSID:	00:03:7F:42:06:AC
SSID Hidden Attribute:	Visual
SSID1 Name:	Atheros XSpan Network
SSID1 Encrypted Status:	None

Situation of Send and Receive Packets :

Interface	Receive				Send			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ath0	0	0	0	0	0	0	756	756

ETHERNET INFORMATION

Home Gateway Information :

IP Address:	192.168.0.1
Net Mask:	255.255.255.0

Situation of Send and Receive Packets :

Interface	Receive				Send			
	Bytes	Pkts	Drops	Errs	Bytes	Pkts	Drops	Errs
Ethernet LAN1	2621359	27522	18	0	27511283	27971	0	0

POWERLINE DEVICES INFORMATION

Network Password: HomePlugAV
Local Device MAC: 00:b0:52:00:00:03
Model: Atheros HomePlug AV Device
Firmware Version: INT6400-MAC-4-2-4203-00-4338-20100721-FINAL-C
Low Power Mode: Normal

Remote devices detected:

Alias	MAC	Model	FIRMWARE	TX (Mbps)	RX (Mbps)	TEI	Low Power Mode
Device1	00:1f:a4:90:d7:12	Atheros HomePlug AV Device	INT7400-MAC-5-2-5203-00-907-20110320-FINAL-D	0	0	3	Normal
Device2	00:12:1a:33:11:3e	Atheros HomePlug AV Device	INT6400-MAC-4-4-4405-00-4497-20101201-FINAL-B	0	0	7	Sleeping/Offline

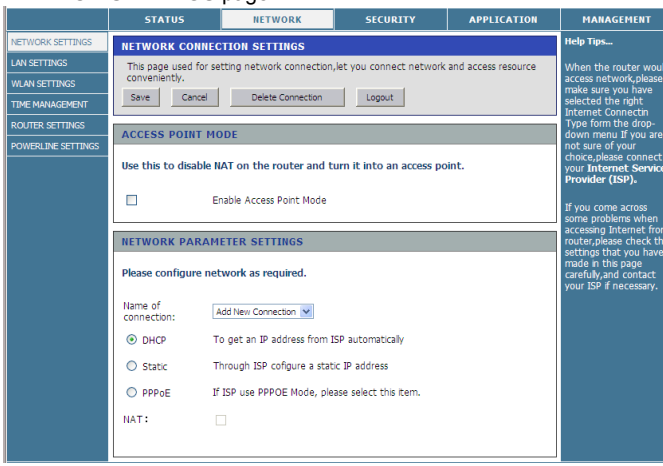
This page shows you the device WLAN interface information, Ethernet information, and PLC device information.

4.2 Network

The submenu of **NETWORK** contains **NETWORK SETTINGS**, **LAN SETTINGS**, **WLAN SETTINGS**, **TIME MANAGEMENT**, **ROUTER SETTINGS**, and **POWERLINE SETTINGS**.

4.2.1 Network Settings

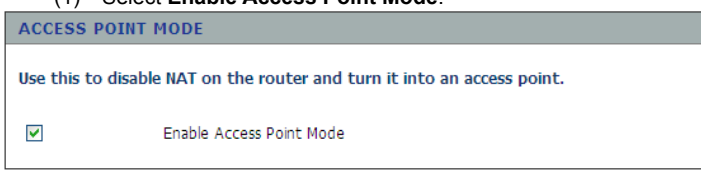
Choose **NETWORK** > **NETWORK SETTINGS** to display the **NETWORK CONNECTION SETTINGS** page.


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
TIME MANAGEMENT
ROUTER SETTINGS
POWERLINE SETTINGS
NETWORK CONNECTION SETTINGS
This page used for setting network connection,let you connect network and access resource conveniently.
Save
Cancel
Delete Connection
Logout
ACCESS POINT MODE
Use this to disable NAT on the router and turn it into an access point.
Enable Access Point Mode
NETWORK PARAMETER SETTINGS
Please configure network as required.
Name of connection:
Add New Connection
DHCP
To get an IP address from ISP automatically
Static
Through ISP cofigure a static IP address
PPPoE
If ISP use PPPOE Mode, please select this item.
NAT:
Help Tips...
When the router would access network,please make sure you have selected the right Internet Connectn Type form the drop-down menu If you are not sure of your choice,please connect your Internet Service Provider (ISP).
If you come across some problems when accessing Internet from router,please check the settings that you have made in this page carefully,and contact your ISP if necessary.

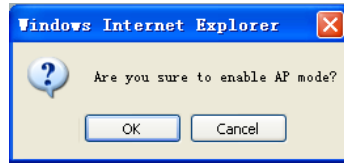
Access point mode

Do as follows to configure the AP mode:

(1) Select **Enable Access Point Mode**.



(2) Click **OK** in the window displayed.



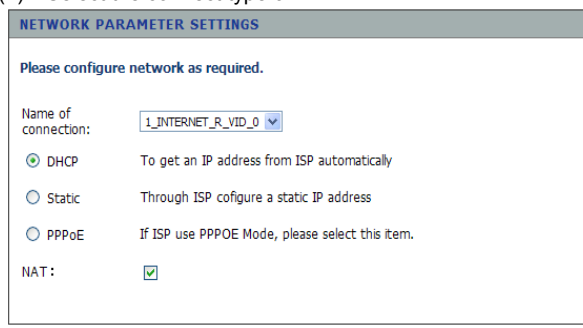
The device now works in the AP mode.

Router mode

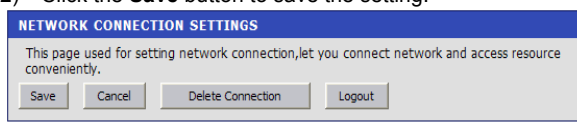
Unselect **Enable Access Point Mode** and the device works in the router mode.

Setting DHCP connection

(1) Select the connect type of **DHCP**.



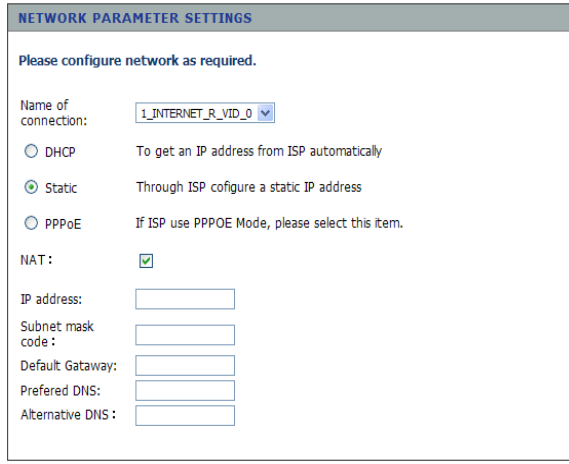
(2) Click the **Save** button to save the setting.



The device will automatically get an IP address from DHCP server.

Setting static connection

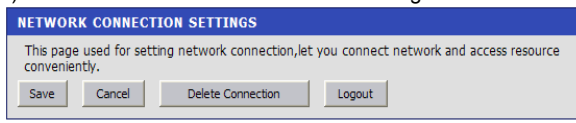
(1) Select the connect type of **Static**.



(2) Enter the following parameters

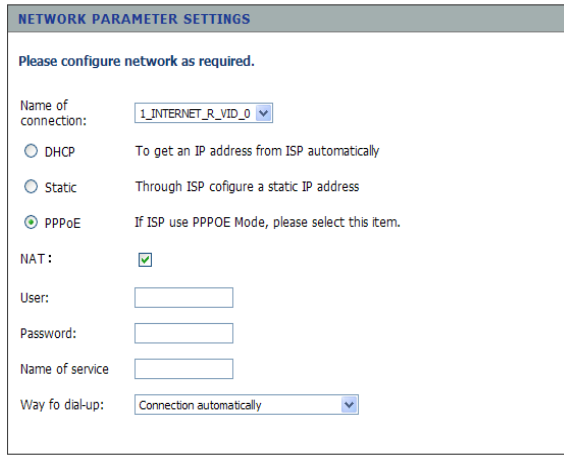
- IP address
- Subnet mask code
- Default Gateway
- Preferred DNS
- Alternative DNS

(3) Click the **Save** button to save the setting.



Setting PPPOE connection

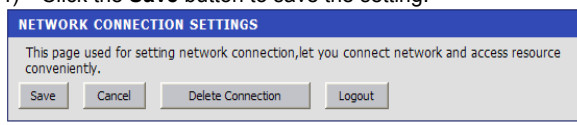
(1) Select the connect type of **PPPOE**.



(2) Enter the user name and password provided by the ISP. If you are not sure of the service name, you can leave it blank.

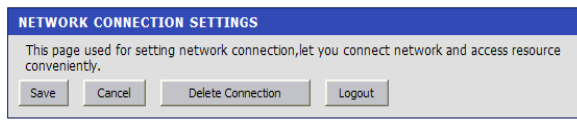
(3) Select the preferred dial-up mode from the drop-down list. The default dialup mode is automatic connection.

(4) Click the **Save** button to save the setting.



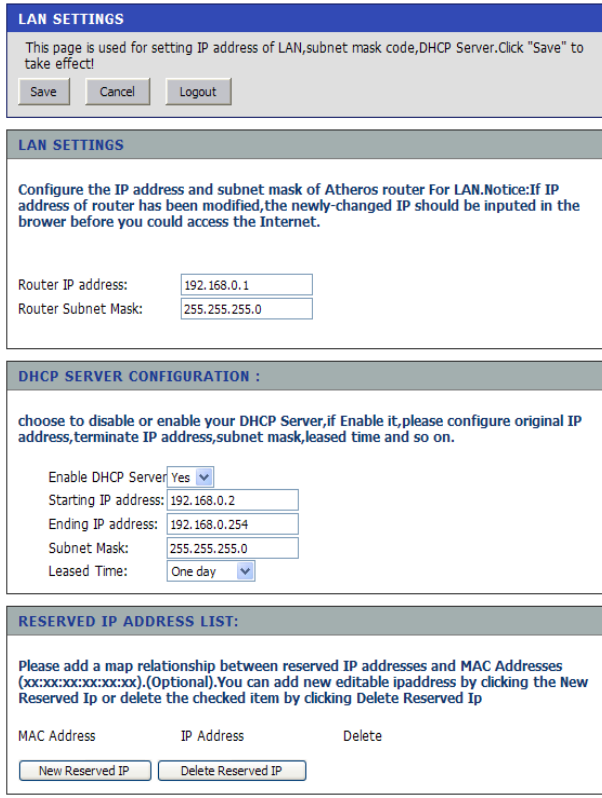
Deleting an internet connection

Click **Delete Connection** to delete an internet connection.



4.2.2 LAN Settings

Choose **NETWORK** > **LAN SETTINGS** to display the **LAN SETTINGS** page.


LAN SETTINGS
This page is used for setting IP address of LAN,subnet mask code,DHCP Server.Click "Save" to take effect!
Save
Cancel
Logout
LAN SETTINGS
Configure the IP address and subnet mask of Atheros router For LAN.Notice:If IP address of router has been modified,the newly-changed IP should be inputed in the brower before you could access the Internet.
Router IP address:
192.168.0.1
Router Subnet Mask:
255.255.255.0
DHCP SERVER CONFIGURATION :
choose to disable or enable your DHCP Server,if Enable it,please configure original IP address,terminate IP address,subnet mask,leased time and so on.
Enable DHCP Server
Yes
Starting IP address:
192.168.0.2
Ending IP address:
192.168.0.254
Subnet Mask:
255.255.255.0
Leased Time:
One day
RESERVED IP ADDRESS LIST:
Please add a map relationship between reserved IP addresses and MAC Addresses (xx:xx:xx:xx:xx:xx).(Optional).You can add new editable ipaddress by clicking the New Reserved Ip or delete the checked item by clicking Delete Reserved Ip
MAC Address
IP Address
Delete
New Reserved IP
Delete Reserved IP

In this page, you can configure the parameters of the LAN port and DHCP server parameters. You can modify the IP address of the LAN port according to the actual network environment.

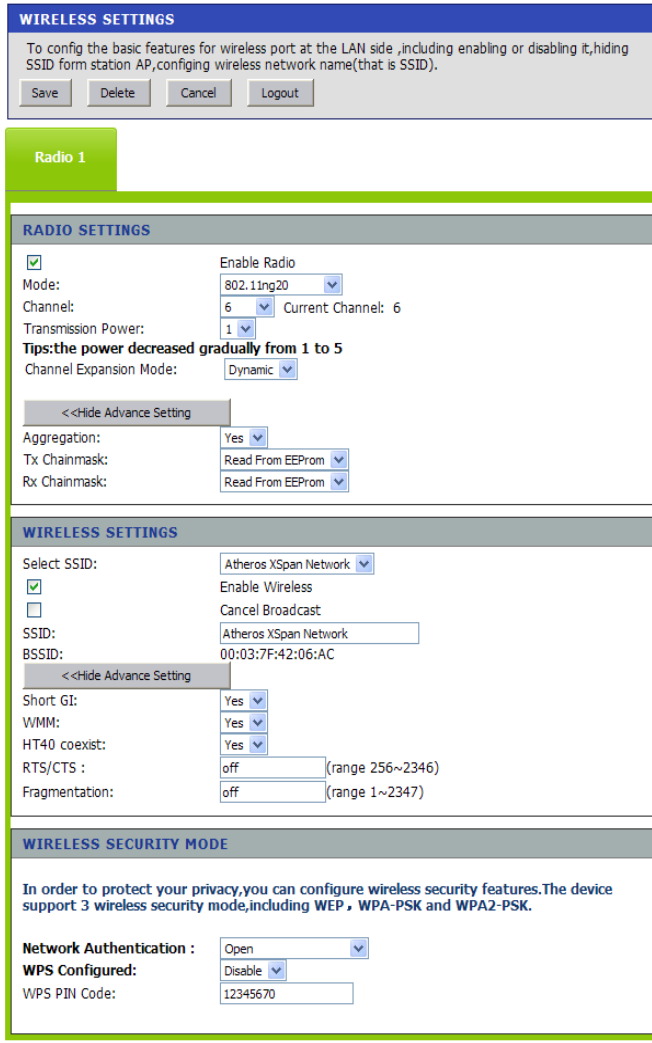
The following table describes parameters and buttons in this page:

Field	Description
Router IP Address	The IP address of the LAN interface. The default IP address is **192.168.0.1**.
Router Subnet Mask	The subnet mask of the IP address of the LAN interface. The default subnet mask is **255.255.255.0**.

Field	Description
Enable DHCP Server	Enable or disable DHCP service.
Starting IP address	The first address in a consecutive IP address pool.
Ending IP address	The last address in a consecutive IP address pool.
Subnet Mask	The subnet mask that the DHCP server assigns.
Leased Time	After the DHCP lease time elapsed, the router automatically assigns new IP addresses for all connected computers.
New Reserved IP	Add a map relationship between the reserved IP address and MAC address. To reserve an IP address: ● Under **Reserved IP address List**, click **New Reserved IP** ● Enter the MAC address and IP address ● Click the **Save** button to save the settings.
Delete Reserved IP	Select an entry of a reserved address and click the button to delete it.

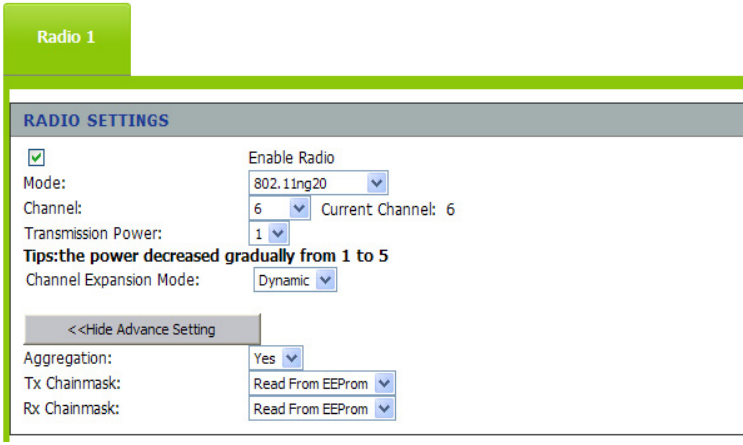
4.2.3 WLAN Settings

Choose **NETWORK** > **WLAN SETTINGS** to display the **WIRELESS SETTINGS** page.


WIRELESS SETTINGS
To config the basic features for wireless port at the LAN side ,including enabling or disabling it,hiding SSID form station AP,configing wireless network name(that is SSID).
Save
Delete
Cancel
Logout
Radio 1
RADIO SETTINGS
Enable Radio
Mode:
802.11ng20
Channel:
6
Current Channel: 6
Transmission Power:
1
Tips:the power decreased gradually from 1 to 5
Channel Expansion Mode:
Dynamic
<<Hide Advance Setting
Aggregation:
Yes
Tx Chainmask:
Read From EEProm
Rx Chainmask:
Read From EEProm
WIRELESS SETTINGS
Select SSID:
Atheros XSpan Network
Enable Wireless
Cancel Broadcast
SSID:
Atheros XSpan Network
BSSID:
00:03:7F:42:06:AC
<<Hide Advance Setting
Short GI:
Yes
WMM:
Yes
HT40 coexist:
Yes
RTS/CTS :
off
(range 256~2346)
Fragmentation:
off
(range 1~2347)
WIRELESS SECURITY MODE
In order to protect your privacy,you can configure wireless security features.The device support 3 wireless security mode,including WEP，WPA-PSK and WPA2-PSK.
Network Authentication :
Open
WPS Configured:
Disable
WPS PIN Code:
12345670

4.2.3.1 Radio settings

In this page, you may set parameters of the wireless mode, channel, and transmission power.



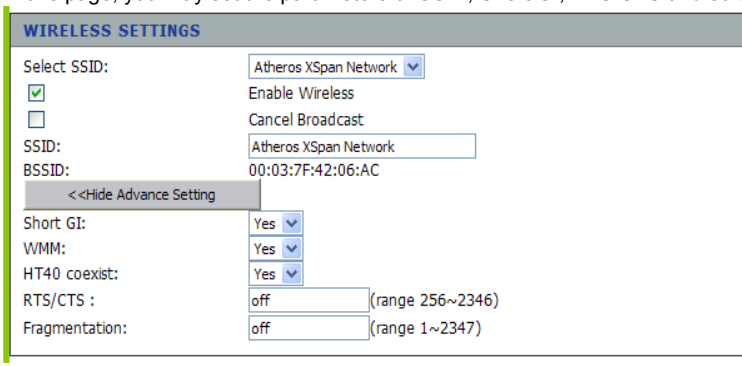
The following table describes parameters in this page:

Field	Description
Enable Radio	Enable or disable the wireless LAN interface.
Mode	Select the appropriate wireless mode. 802.11ng20 802.11b Only 802.11g 802.11ng20 802.11ng40plus 802.11ng40minus
Channel	Select the working channel of the wireless network. The default channel is channel 6.
Transmission Power	Set transmit power. The default is **1**, that is, the greatest transmit power.
Channel Expansion Mode	Select a channel mode from the drop-down list. ● Dynamic (default) ● Static

Field	Description
Aggregation	Enable or disable A-MSDU. MSDU is the aggregation of multiple MSDUs by using certain method and the multiple MSDUs forms a greater load.
Tx Chainmask	The stream number mask of wireless antenna transmits.
Rx Chainmask	The stream number mask of wireless antenna receivers.

4.2.3.2 Wireless Settings

In this page, you may set the parameters of SSID, Short GI, RTS/CTS and so on.



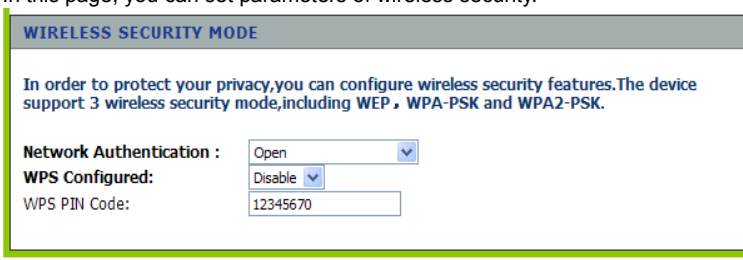
The following table describes parameters in this page:

Field	Description
Select SSID	Select an SSID from the drop-down list.
Enable Wireless	Enable or disable the wireless function for the selected SSID.
Cancel Broadcast	Enable or disable SSID broadcast. If it is enabled, the device broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the corresponding wireless network.
SSID	Network name. The SSID can contain up to 32

Field	Description
	characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive.
BSSID	The MAC address of the wireless interface.
Short GI	Set the short guard interval. You may select **Yes** or **No**. The default guard interval is set to **Yes**. ● Yes: guard interval 400us ● No: guard interval 800us
WMM	Enable or disable WMM. After WMM is enabled, AP can process different types of wireless data by their priority levels.
HT40 coexist	You may select **Yes** or **No**. The default coexist is **No**.
RTS/CTS	Set the CTS/RTS threshold. The default RTS threshold is off. The value ranges from 256 to 2346.
Fragmentation	The default fragment threshold is off. The value ranges from 1 to 2347.

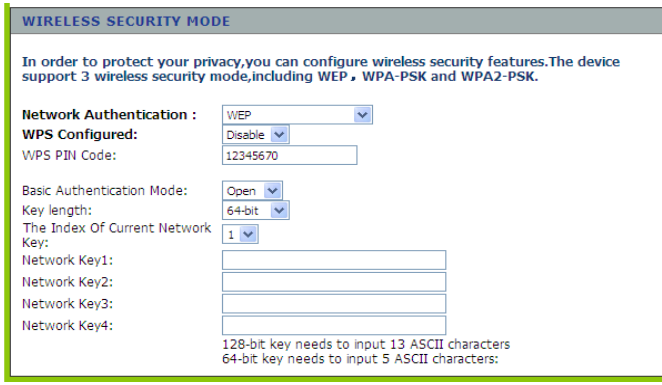
4.2.3.3 Wireless Security Mode

In this page, you can set parameters of wireless security.


WIRELESS SECURITY MODE
In order to protect your privacy,you can configure wireless security features.The device support 3 wireless security mode,including WEP，WPA-PSK and WPA2-PSK.
Network Authentication :
Open
WPS Configured:
Disable
WPS PIN Code:
12345670

In order to protect your privacy, you can configure wireless security, including WEP, WPA-PSK, WPA2-PSK, and 802.1X.

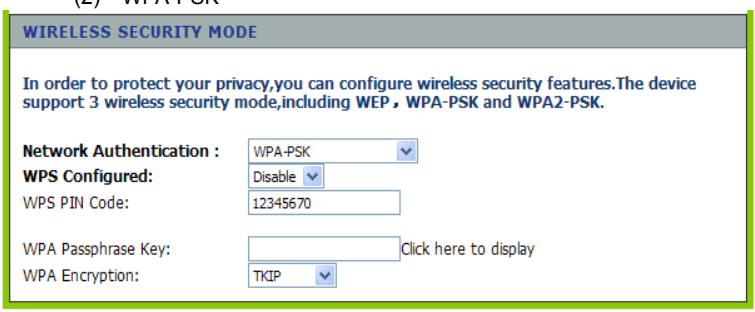
(1) WEP



The following table describes parameters in this page:

Field	Description
Basic Authentication Mode	You can select **Open**, **Share**, and **Both**.
Key length	Select the length of a key. You can select 64-bit,128-bit and 152-bit
The Index of Current Network Key	Select an index as the WEP key.
Network Key (1/2/3/4)	64-bit : 10 Hex or 5 ASCII characters. 128-bit: 26 Hex or 13 ASCII characters. 152-bit: 32 Hex or 16 ASCII characters.

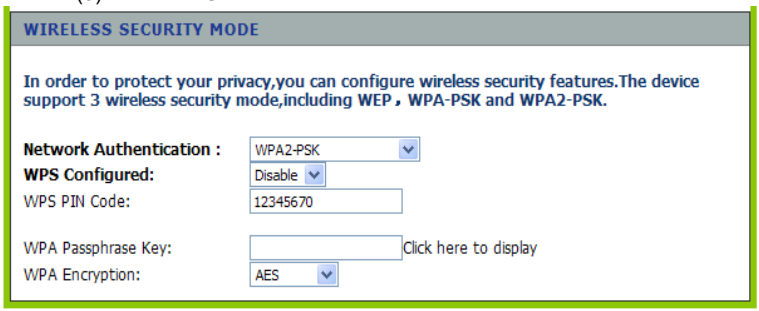
(2) WPA-PSK



The following table describes parameters in this page:

Field	Description
WPA Passphrase Key	Enter 8 to 63 ASCII characters or no more than 64 hexadecimal numbers
WPA Encryption	Select **TKIP , AES** or **TKIP AES**.

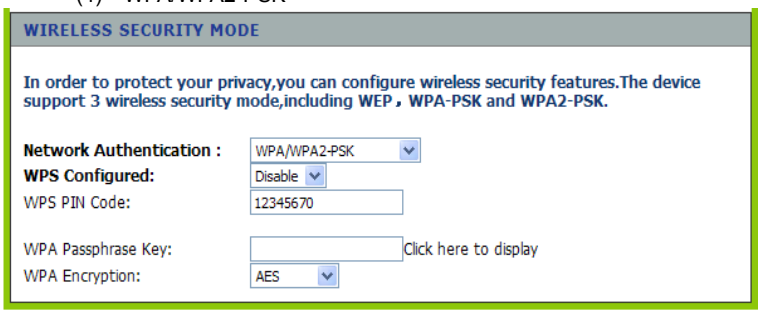
(3) WPA2-PSK



The following table describes parameters in this page:

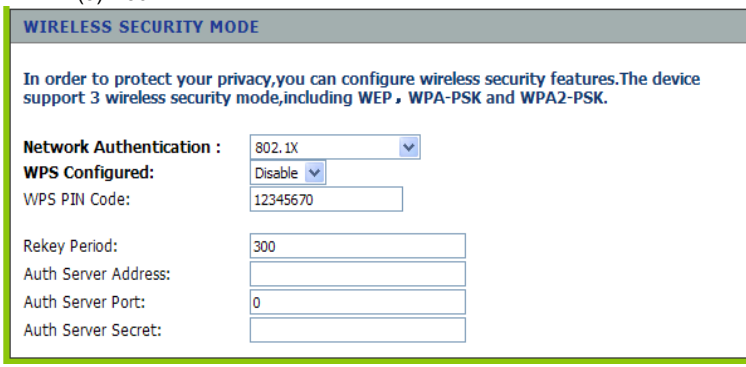
Field	Description
WPA Passphrase Key	Enter 8 to 63 ASCII characters or no more than 64 hexadecimal numbers
WPA Encryption	Select **TKIP , AES** or **TKIP AES**.

(4) WPA/WPA2-PSK



For parameter descriptions, refer to **WPA-PSK**.

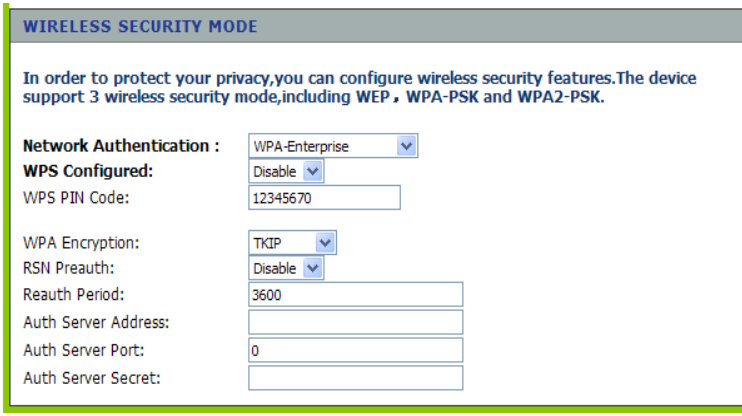
(5) 802.1X



The following table describes parameters in this page:

Field	Description
Rekey Period	Defines the period after which new keys will be issued to prospective originators.
Auth Server Address	The IP address of the RADIUS server.
Auth Server Port	The default port number is 1812. You may change it according to the server setting.
Auth Server Secret	The key that the RADIUS server needs for authentication.

(6) WPA-Enterprise, WPA2-Enterprise, or WPA/WPA2-Enterprise



The following table describes parameters in this page:

Field	Description
WPA Encryption	Select **TKIP**, **AES**, or **TKIP AES**.
RSN Preauth	Robust Security Network (RSN), define the key generation and distribution. This function is disabled by default.
Reauth Period	Defines the period for Reauth.
Auth Server Address	The IP address of the RADIUS server.
Auth Server Port	The default port number is 1812. You may change it according to the server setting.
Auth Server Secret	The key that the RADIUS server needs for authentication.

WPS Progress

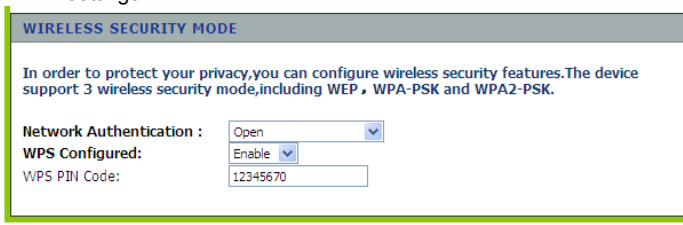
WPS modes include PIN and PBC modes. WPS supports two operation modes, including the **Enrollee** and **PBC** mode. The **Enrollee** mode needs to apply PIN code negotiation.

- Enrollee Mode

Step 1 Select **Enrollee** mode on the wireless client and the software of wireless client will generate a random PIN code, for example, 12345670.

Step 2 Enter the PIN code of the wireless client (for example, 12345670) in the **WIRELESS SETTINGS** page.

Step 3 Click the **Save** button on the **WIRELESS SETTINGS** page to save settings.


WIRELESS SECURITY MODE
In order to protect your privacy,you can configure wireless security features.The device support 3 wireless security mode,including WEP，WPA-PSK and WPA2-PSK.
Network Authentication :
Open
WPS Configured:
Enable
WPS PIN Code:
12345670

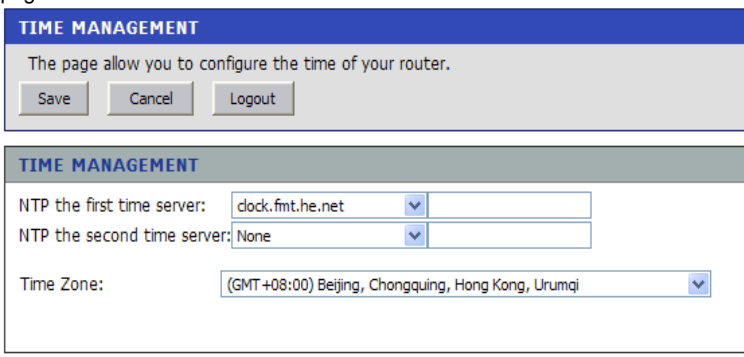
- PBC Mode

Step 1 Press the **WPS** button on the device's panel.

Step 2 Enable the PBC function on the wireless client. In that case, PLV-200AV-PEWN and the wireless client will automatically establish connection.

4.2.4 Time Management

Choose **NETWORK** > **TIME MANAGEMENT** to display the **TIME MANAGEMENT** page.



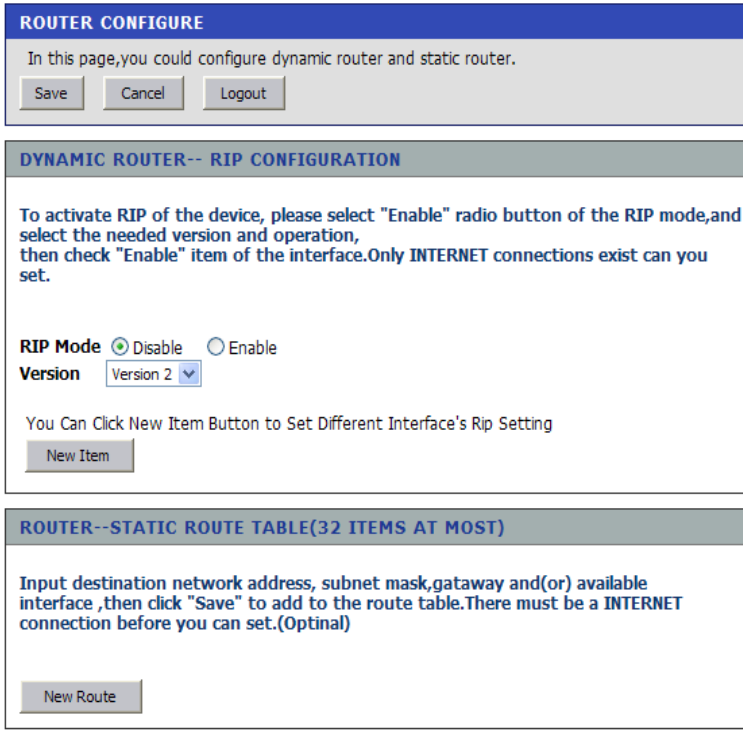
The following table describes parameters in this page:

Field	Description

Field	Description
NTP first time server	Select an NTP first time server from the drop-down list. Or select other and enter the URL address of the time server manually.
NTP second time server	Select an NTP second time server from the drop-down list. Or select other and enter the URL address of the time server manually.
Time Zone	Select the time zone from the drop-down list.

4.2.5 Router Settings

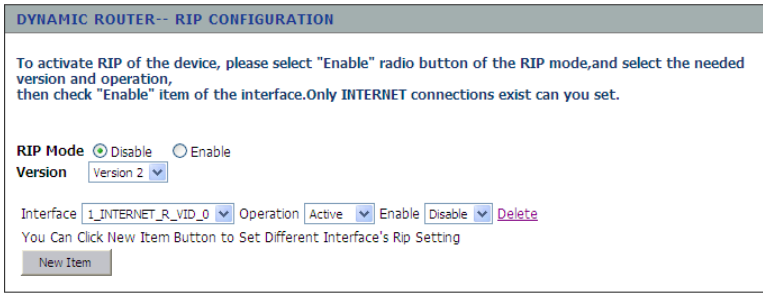
Choose **NETWORK** > **ROUTER SETTINGS** to display the **ROUTER SETTINGS** page.


ROUTER CONFIGURE
In this page,you could configure dynamic router and static router.
Save
Cancel
Logout
DYNAMIC ROUTER-- RIP CONFIGURATION
To activate RIP of the device, please select "Enable" radio button of the RIP mode,and select the needed version and operation,
then check "Enable" item of the interface.Only INTERNET connections exist can you set.
RIP Mode
Disable
Enable
Version
Version 2
You Can Click New Item Button to Set Different Interface's Rip Setting
New Item
ROUTER--STATIC ROUTE TABLE(32 ITEMS AT MOST)
Input destination network address, subnet mask,gataway and(or) available interface ,then click "Save" to add to the route table.There must be a INTERNET connection before you can set.(Optinal)
New Route

In this page, you can configure the dynamic router and static router.

4.2.5.1 Dynamic Route

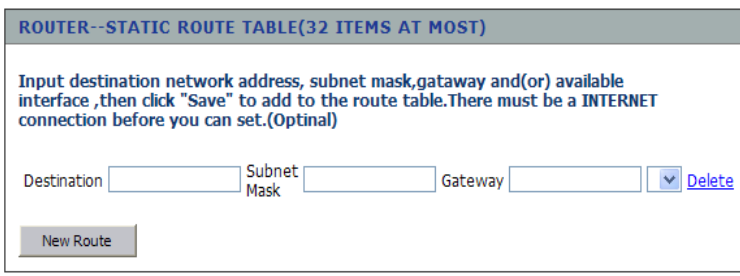
Click **New Item** to display the following page.



The following table describes parameters in this page:

Field	Description
RIP Mode	Enable or Disable the RIP mode.
Version	RIP1 broadcasts a route to discover and maintain routing tables. RIP2 can be broadcast or multicast routing approach to discover and maintain routing tables. If the network approach to optimize the use of CIDR IP address allocation, it can only be used RIP2, RIP1 does not support CIDR
Operation	Select **Active** or **Passive**. ● Active: Routers advertise their routes to other routers. ● Passive: The passive router receives notice and updates its routing accordingly.

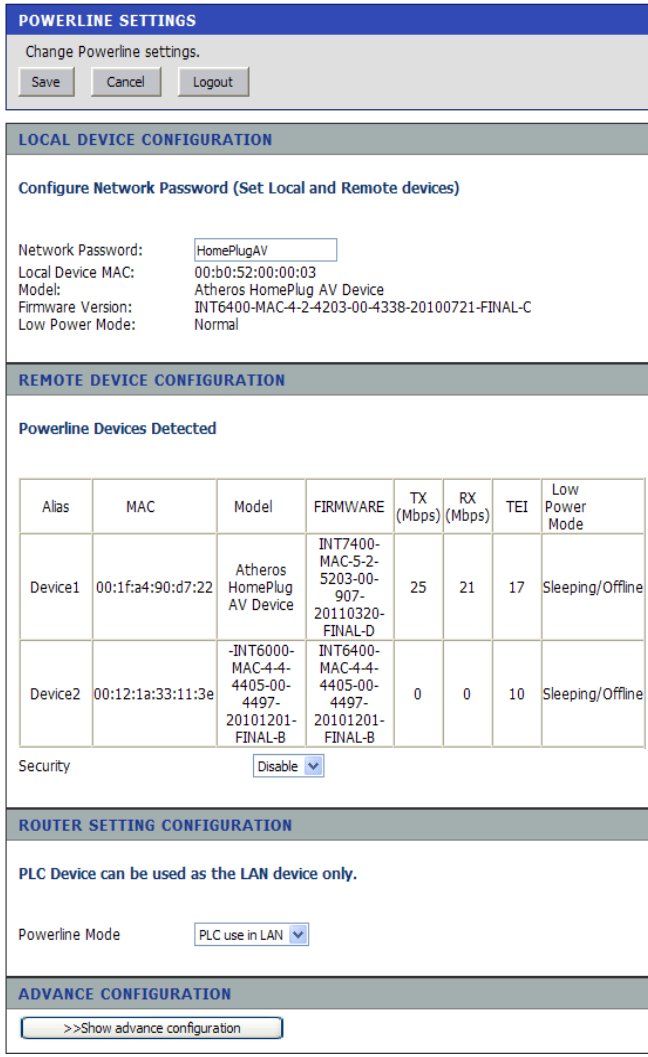
4.2.5.2 Static Route


ROUTER--STATIC ROUTE TABLE(32 ITEMS AT MOST)
Input destination network address, subnet mask,gataway and(or) available interface ,then click "Save" to add to the route table.There must be a INTERNET connection before you can set.(Optinal)
Destination
Subnet Mask
Gateway
Delete
New Route

In this page, enter the destination IP address, subnet mask, and the gateway provided by you ISP.

4.2.6 Powerline Settings

Choose **NETWORK** > **POWERLINE SETTINGS** to display the **POWERLINE SETTINGS** page.



POWERLINE SETTINGS

Change Powerline settings.

Save | Cancel | Logout

LOCAL DEVICE CONFIGURATION

Configure Network Password (Set Local and Remote devices)

Network Password:	HomePlugAV
Local Device MAC:	00:b0:52:00:00:03
Model:	Atheros HomePlug AV Device
Firmware Version:	INT6400-MAC-4-2-4203-00-4338-20100721-FINAL-C
Low Power Mode:	Normal

REMOTE DEVICE CONFIGURATION

Powerline Devices Detected

Alias	MAC	Model	FIRMWARE	TX (Mbps)	RX (Mbps)	TEI	Low Power Mode
Device1	00:1f:a4:90:d7:22	Atheros HomePlug AV Device	INT7400-MAC-5-2-5203-00-907-20110320-FINAL-D	25	21	17	Sleeping/Offline
Device2	00:12:1a:33:11:3e	-INT6000-MAC-4-4-4405-00-4497-20101201-FINAL-B	INT6400-MAC-4-4-4405-00-4497-20101201-FINAL-B	0	0	10	Sleeping/Offline

Security: Disable

ROUTER SETTING CONFIGURATION

PLC Device can be used as the LAN device only.

Powerline Mode: PLC use in LAN

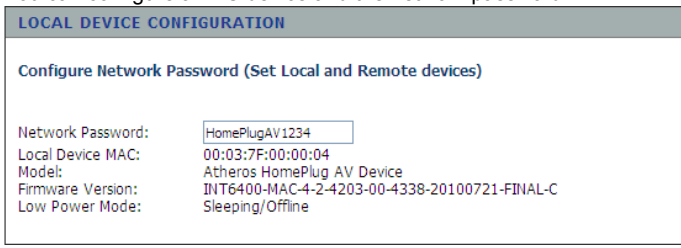
ADVANCE CONFIGURATION

>>Show advance configuration

In this page, you can change powerline settings.

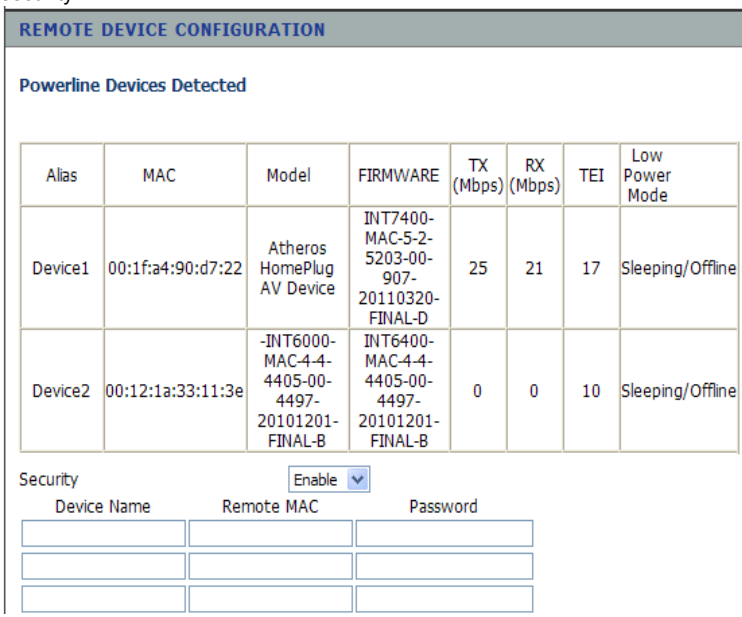
4.2.6.1 Local Device Configure

You can configure a PLC device and the network password.



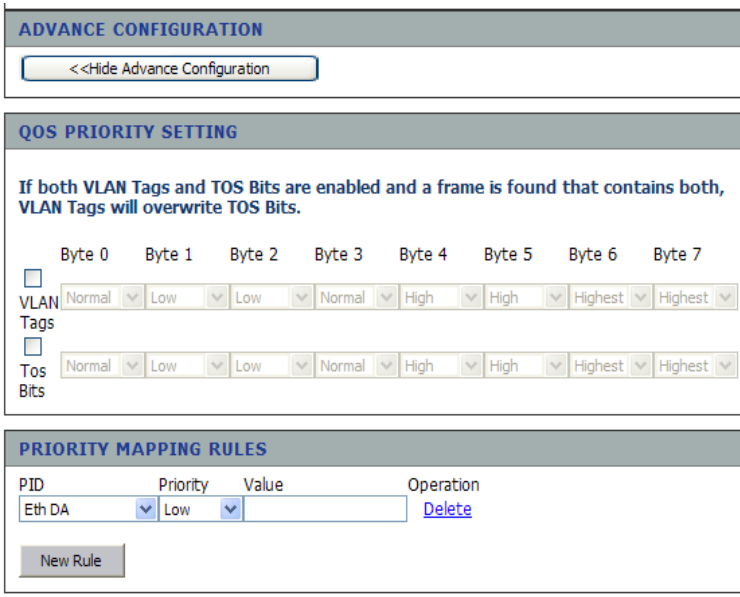
4.2.6.2 Remote Device Configure

In this page, you can view the remote device list and set the remote device security.



Set **Security** to **Enable** and you can set the password and MAC address for a remote device. Users can set up to eight devices at one time.

4.2.6.3 Advance Configuration


ADVANCE CONFIGURATION
<<Hide Advance Configuration
QOS PRIORITY SETTING
If both VLAN Tags and TOS Bits are enabled and a frame is found that contains both, VLAN Tags will overwrite TOS Bits.
Byte 0 Byte 1 Byte 2 Byte 3 Byte 4 Byte 5 Byte 6 Byte 7
VLAN Tags
Normal Low Low Normal High High Highest Highest
Tos Bits
Normal Low Low Normal High High Highest Highest
PRIORITY MAPPING RULES
PID Priority Value Operation
Eth DA Low
Delete
New Rule

The PLC QOS setting is only for traffic on the PLC, not for the whole router or AP's QOS. It contains VLAN tags and TOS bits. Each VLAN tag or TOS bit has eight bits to identify the QOS settings, and four levels are available. By default the QOS setting is disabled:

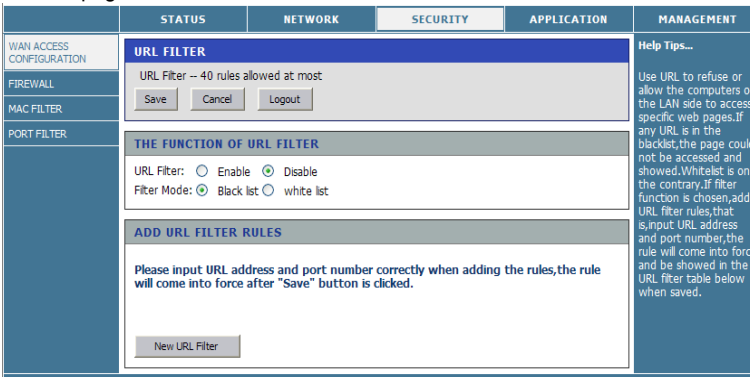
Under the priority mapping rules section, classify a special flow to a certain priority by clicking the **New Rule** button to generate a new configuration item to edit. Click the **Save** button to save the settings.

4.3 Security

The submenu of **SECURITY** contains **WAN ACCESSS CONFIGURATION**, **FIREWALL**, **MAC FILTER**, and **PORT FILTER**.

4.3.1 WAN Access Configuration

Choose **SECURITY** > **WAN ACCESSS CONFIGURATION** to display the **URL FILTER** page.

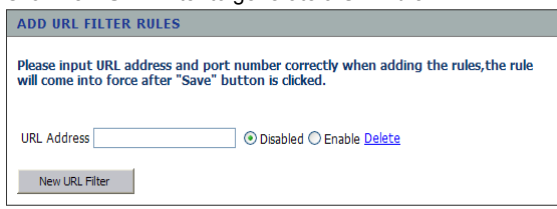

STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
WAN ACCESS CONFIGURATION
FIREWALL
MAC FILTER
PORT FILTER
URL FILTER
URL Filter -- 40 rules allowed at most
Save
Cancel
Logout
THE FUNCTION OF URL FILTER
URL Filter: Enable Disable
Filter Mode: Black list white list
ADD URL FILTER RULES
Please input URL address and port number correctly when adding the rules,the rule will come into force after "Save" button is clicked.
New URL Filter
Help Tips...
Use URL to refuse or allow the computers of the LAN side to access specific web pages.If any URL is in the blacklist,the page could not be accessed and showed.Whitelist is on the contrary.If filter function is chosen,add URL filter rules,that is,input URL address and port number,the rule will come into force and be showed in the URL filter table below when saved.

Enable URL Filter and select Black list or White list. Click the **Save** button to save the settings.

- **Black List**: Indicates to prevent data that complies with the rule from passing through.
- **White List**: Indicates to allow data that complies with the rule to pass through only.

Do as follows to add a URL filter rule:

Step 1 Click **New URL** Filter to generate a URL rule.

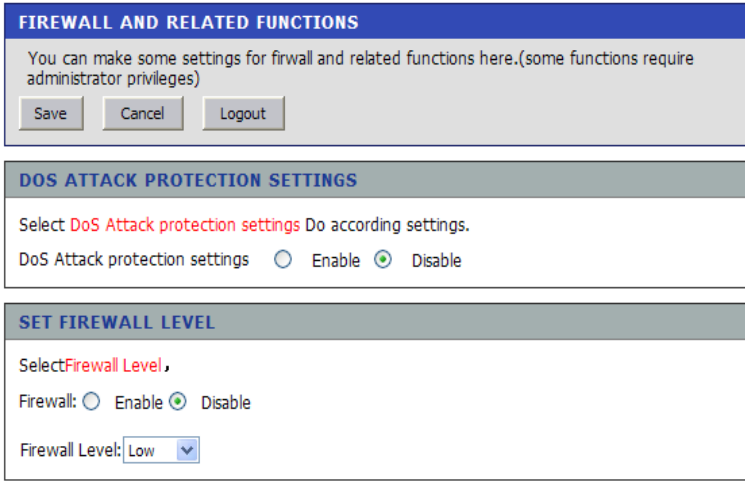

ADD URL FILTER RULES
Please input URL address and port number correctly when adding the rules,the rule will come into force after "Save" button is clicked.
URL Address
Disabled Enable Delete
New URL Filter

Step 2 Enter a URL in the URL Address field.

Step 3 Click **Save** to save the settings.

4.3.2 Firewall

Choose **SECURITY** > **FIREWALL** to display the **FIREWALL AND RELEATED FUNCTIONS** page.

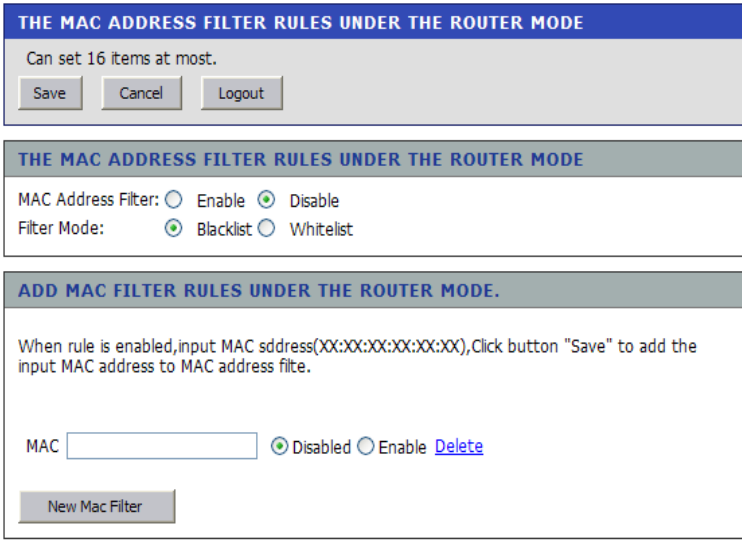


The following table describes parameters in this page:

Field	Description
Firewall Level	● Low: You can use all service in the gateway from the WAN side. ● Middle: You cannot use TCP (1~1024 port) and UDP (1~66, 69~1024 port). Therefore, you cannot use the following frequently-used service: FTP (21), Telnet(23), Http(80), Rip(520) from the WAN side. ● High: You cannot use TCP (1~1024 port) and UDP (1~66, 69~1024 port). Therefore, you cannot use the following service: FTP (21), Telnet(23), Http(80), Rip(520), zebra(2601) from the WAN side.

4.3.3 MAC Filter

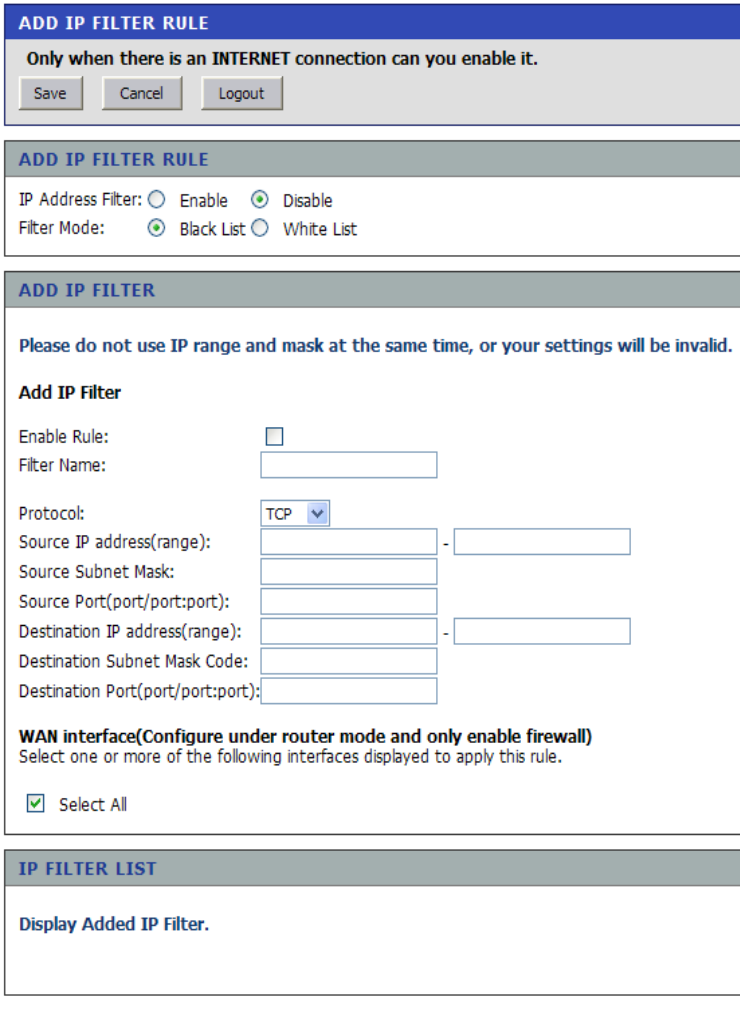
Choose **SECURITY** > **WAC FILTER** to display the **THE MAC ADDRESS FILTER RULES UNDER THE ROUTER MODE** page.


THE MAC ADDRESS FILTER RULES UNDER THE ROUTER MODE
Can set 16 items at most.
Save
Cancel
Logout
THE MAC ADDRESS FILTER RULES UNDER THE ROUTER MODE
MAC Address Filter: Enable Disable
Filter Mode: Blacklist Whitelist
ADD MAC FILTER RULES UNDER THE ROUTER MODE.
When rule is enabled,input MAC sddress(XX:XX:XX:XX:XX:XX),Click button "Save" to add the input MAC address to MAC address filte.
MAC
Disabled Enable Delete
New Mac Filter

In this page, you can enable or disable the MAC filter. Enter MAC address in the text field and click **Save** to add the address to the MAC list. The format of MAC address is *xx:xx:xx:xx:xx:xx* (x is a hexadecimal value ranging from 0~9 or A~F).

4.3.4 Port Filter

Choose **SECURITY** > **PORT FILTER** to display the **ADD IP FILTER RULE** page.


ADD IP FILTER RULE
Only when there is an INTERNET connection can you enable it.
Save
Cancel
Logout
ADD IP FILTER RULE
IP Address Filter: Enable Disable
Filter Mode: Black List White List
ADD IP FILTER
Please do not use IP range and mask at the same time, or your settings will be invalid.
Add IP Filter
Enable Rule:
Filter Name:
Protocol: TCP
Source IP address(range):
Source Subnet Mask:
Source Port(port/port:port):
Destination IP address(range):
Destination Subnet Mask Code:
Destination Port(port/port:port):
WAN interface(Configure under router mode and only enable firewall)
Select one or more of the following interfaces displayed to apply this rule.
Select All
IP FILTER LIST
Display Added IP Filter.

In this page, you can enable or disable the IP filter.

The following table describes parameters in this page:

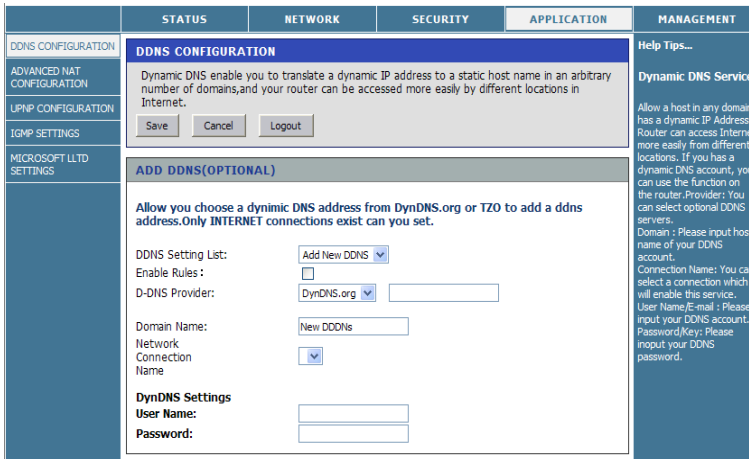
Field	Description
IP Address Filter	Select **Enable** or **Disable**.
Filter Mode	Select Black List or White List.
Protocol	You can select TCP, UDP, or ICMP.
Source IP Address	Enter the source IP Address range, for example 192.168.0.100~192.168.0.200.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a port number or a port range to define the access to the Internet. If this parameter is left blank, all ports will be refused or allowed according to the filer rule.
Destination IP Address	Enter the destination IP address range.

4.4 Application

The submenu of **APPLICATION** contains **DDNS CONFIGURATION**, **ADVANCED NAT CONFIGURATION**, **UPNP CONFIGURATION**, **IGMP CONFIGURATION**, and **MICROSOFT LLTD SETTINGS**.

4.4.1 DDNS Configuration

Choose **APPLICATION** > **DDNS CONFIGURATION** to display the **DDNS CONFIGURATION** page.


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
DDNS CONFIGURATION
ADVANCED NAT CONFIGURATION
UPNP CONFIGURATION
IGMP SETTINGS
MICROSOFT LLTD SETTINGS
DDNS CONFIGURATION
Dynamic DNS enable you to translate a dynamic IP address to a static host name in an arbitrary number of domains,and your router can be accessed more easily by different locations in Internet.
Save
Cancel
Logout
ADD DDNS(OPTIONAL)
Allow you choose a dynimic DNS address from DynDNS.org or TZO to add a ddns address.Only INTERNET connections exist can you set.
DDNS Setting List:
Add New DDNS
Enable Rules:
D-DNS Provider:
DynDNS.org
Domain Name:
New DDDNs
Network Connection Name
DynDNS Settings
User Name:
Password:
Help Tips...
Dynamic DNS Service
Allow a host in any domain has a dynamic IP Address. Router can access Internet more easily from different locations. If you has a dynamic DNS account, you can use the function on the router.Provider: You can select optional DDNS servers.
Domain : Please input host name of your DDNS account.
Connection Name: You can select a connection which will enable this service.
User Name/E-mail : Please input your DDNS account.
Password/Key: Please inoput your DDNS password.

Dynamic DNS (DDNS) is mainly used to realize resolution between fixed domain names and dynamic IP addresses. For a user that uses a dynamic IP address, after the user obtains a new IP address when accessing to the Internet, the dynamic domain name software installed in the host sends the IP address to the dynamic domain name resolution server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Do as follows to add a DDNS provider:

Step 1 Select **Enable Rules**.

Step 2 Select a DDNS provider.

Step 3 Enter the Domain Name, user name, and password.

Step 4 Click **Save** to save the settings.

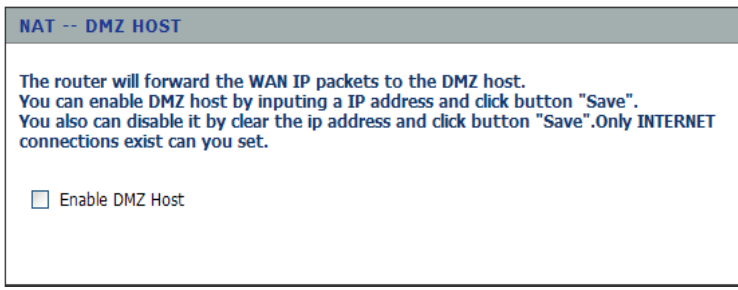
4.4.2 Advanced NAT Configuration

Choose **APPLICATION** > **NAT CONFIGURATION** to display the **ADVANCED NAT CONFIGURATION** page.

ALG configuration

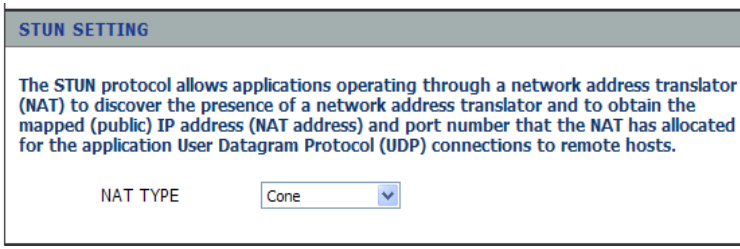
ALG allows customized NAT traversal filters to plug into the gateway to support the address and port translation for application later control/data protocols, such as H.323, real-time streaming protocol (RTSP), layer 2 tunneling protocol (L2TP), IP security (IPSEC) and session initiation protocol (SIP).

NAT-DMZ host


NAT -- DMZ HOST
The router will forward the WAN IP packets to the DMZ host.
You can enable DMZ host by inputing a IP address and click button "Save".
You also can disable it by clear the ip address and click button "Save".Only INTERNET connections exist can you set.
Enable DMZ Host

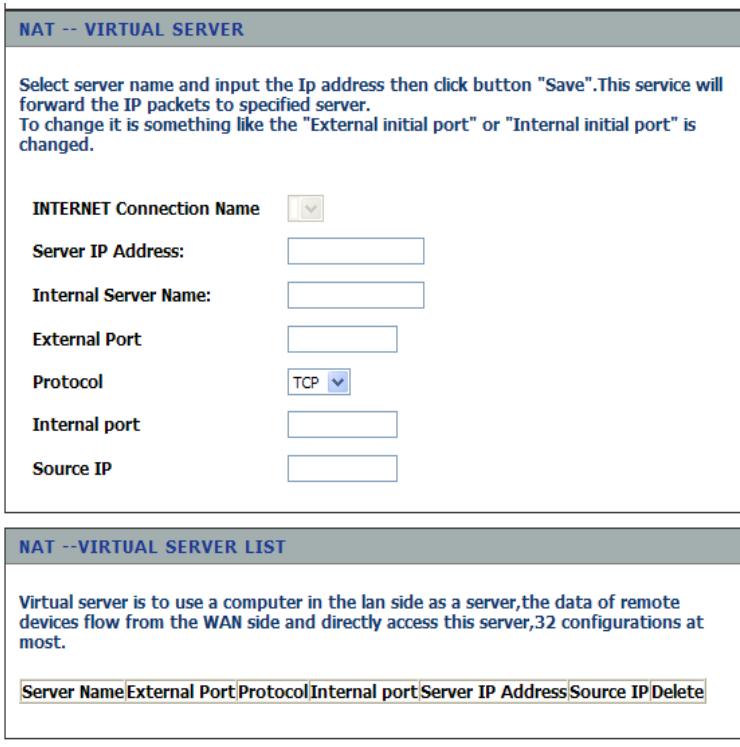
DMZ (Demilitarized Zone) aims to solve the problem that external network can not access internal server behind firewall if you enable DMZ host. The router will forward the WAN IP packets to the DMZ host. But this also makes the computer face security risks, so this is the last resort.

STUN setting


STUN SETTING
The STUN protocol allows applications operating through a network address translator (NAT) to discover the presence of a network address translator and to obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application User Datagram Protocol (UDP) connections to remote hosts.
NAT TYPE
Cone

The STUN protocol allows applications operating through a network address translator (NAT) to discover the presence of a network address translator and to obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application User Datagram Protocol (UDP) connections to remote hosts.

NAT-Virtual server


NAT -- VIRTUAL SERVER
Select server name and input the Ip address then click button "Save".This service will forward the IP packets to specified server.
To change it is something like the "External initial port" or "Internal initial port" is changed.
INTERNET Connection Name
Server IP Address:
Internal Server Name:
External Port
Protocol
TCP
Internal port
Source IP
NAT --VIRTUAL SERVER LIST
Virtual server is to use a computer in the lan side as a server,the data of remote devices flow from the WAN side and directly access this server,32 configurations at most.
Server Name
External Port
Protocol
Internal port
Server IP Address
Source IP
Delete

Do as follows to add a virtual server:

Step 1 Enter the server IP address.

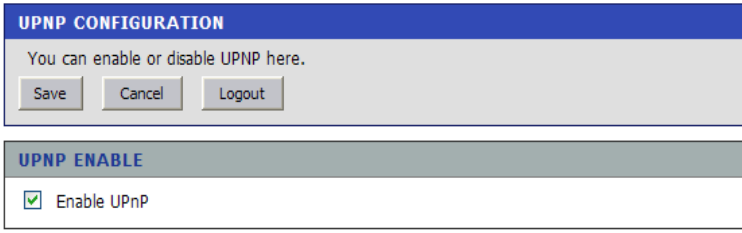
Step 2 Enter the internal server name

Step 3 Specify the external port, protocol, internal port, and source IP.

Step 4 Click **Save** to save the settings and the **NAT-Virtual Server list** will display the virtual server list

4.4.3 UPnP Configuration

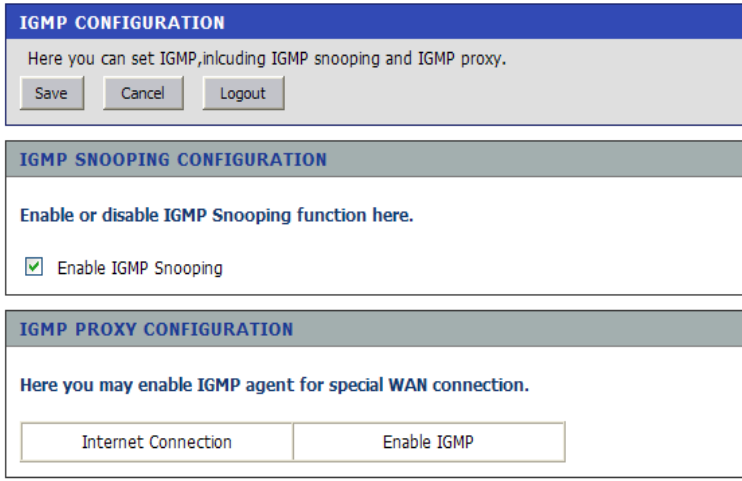
Choose **APPLICATION** > **UPNP CONFIGURATION** to display the **UPNP CONFIGURATION** page.



You can enable or disable UPNP (Universal Plug and Play).

4.4.4 IGMP Settings

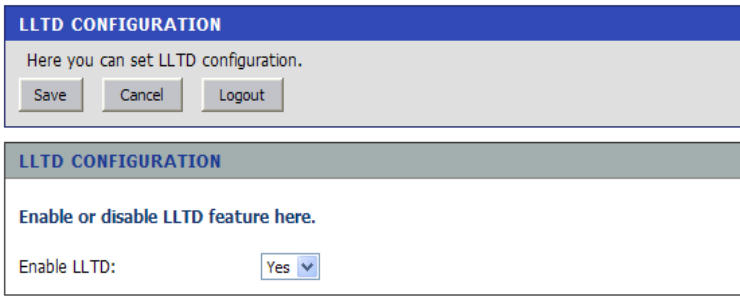
Choose **APPLICATION** > **IGMP SETTINGS** to display the **IGMP SETTINGS** page.



IGMP Snooping is used for multicast management and control.
IGMP proxying enables a PC in the LAN to receive desired multicast traffic from the Internet. Disable IGMP proxying if you do not need this function.

4.4.5 Microsoft LLTD Settings

Choose **APPLICATION** > **MICROSOFT LLTD CONFIGURATION** to display the **LLTD CONFIGURATION** page.



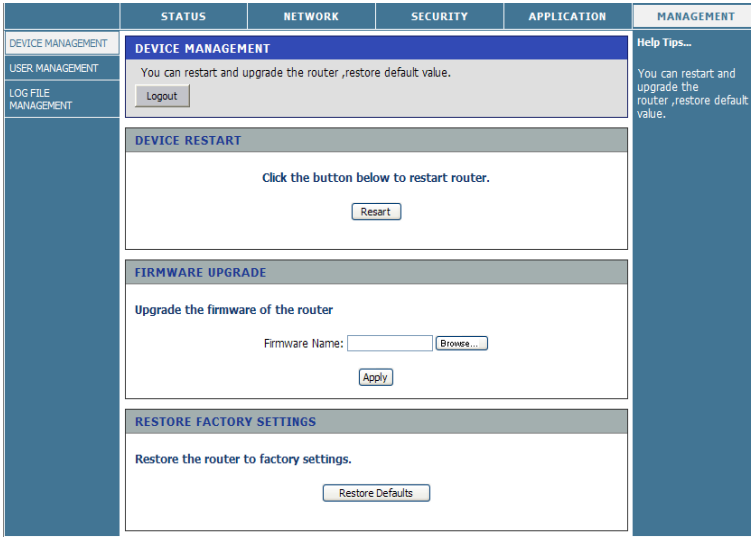
LLTD (Link Layer Topology Discovery), Windows Vista automatically discovers other device's link topology, and these devices are also compatible with LLTD.

4.5 Management

The submenu of **MANAGEMENT** contains **DEVICE MANAGEMNT**, **USER MANAGEENT**, and **LOG FILE MANAGEMENT**.

4.5.1 Device Management

Choose **MANAGEMENT** > **DEVICE MANAGEMNT** to display the **DEVICE MANAGEMNT** page.

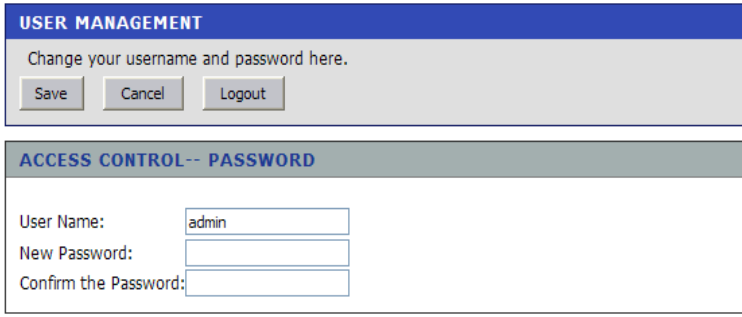


The following table describes parameters in this page:

Field	Description
Restart	Click the Restart button to restart the device.
Update the firmware	If you want to upload the firmware of the device, click **Browse** to choose the new firmware and then click **Apply**. The system begins to upgrade the firmware.
Restore Defaults	Click the Load Default button, the system returns to the factory default settings.

4.5.2 User Management

Choose **MANAGEMENT** > **USER MANAGEMNT** to display the **USER MANAGEMNT** page.



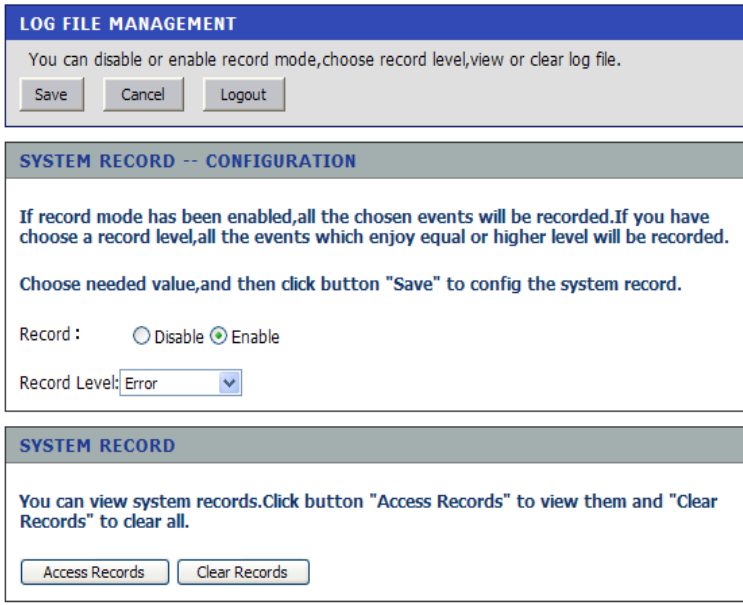
Set the user name and password in this page.

Note:

For security, it is strongly recommended to change the default user name and password. If you forget the password, you can press the Reset button to restore the device to the default settings. The default user name and password are **admin** and **admin** respectively.

4.5.3 Log File Management

Choose **MANAGEMENT** > **LOG FILE MANAGEMNT** to display the **LOG FILE MANAGEMNT** page.


LOG FILE MANAGEMENT
You can disable or enable record mode,choose record level,view or clear log file.
Save
Cancel
Logout
SYSTEM RECORD -- CONFIGURATION
If record mode has been enabled,all the chosen events will be recorded.If you have choose a record level,all the events which enjoy equal or higher level will be recorded.
Choose needed value,and then click button "Save" to config the system record.
Record :
Disable
Enable
Record Level:
Error
SYSTEM RECORD
You can view system records.Click button "Access Records" to view them and "Clear Records" to clear all.
Access Records
Clear Records

If the record mode is enabled and a record level is selected, the events with the set level or higher are recorded.

Click **Access Records** and the log information page is displayed.

Manufacturer:
ProductClass:
SerialNumber:
IP:192.168.1.1
HWVer:
SWVer:
1970-01-01 00:00:14 [Error] (none) daemon.err miniupnpd[1051]: setsockopt(udp, IP_ADD_MEMBERSHIP): No such device
1970-01-01 00:00:14 [Error] (none) daemon.err miniupnpd[1051]: setsockopt(udp_notify, IP_MULTICAST_IF): Cannot assign requested address
1970-01-01 00:00:14 [Error] (none) daemon.err miniupnpd[1051]: Failed to open sockets for sending SSDP notify messages. EXITING
1969-12-31 16:00:23 [Error] (none) daemon.err miniupnpd[3624]: Unable to open pidfile for writing /var/run/miniupnpd.pid: File exists
1969-12-31 22:55:21 [Error] (none) daemon.err miniupnpd[3624]: sendto(udp): Network is unreachable
1969-12-31 22:55:21 [Error] (none) daemon.err miniupnpd[3624]: sendto(udp): Network is unreachable

5 How to Use the Security Pushbutton

This chapter describes how to use the security pushbutton to add new devices to or remove devices from a HomePlug AV logical network (AVLN).

You can monitor the operation progress and outcome by observing the Power LED status.

5.1 Forming a HomePlug AV logical network

When two devices with different NMK values are connected to the same powerline, do as follows to form a logical network:

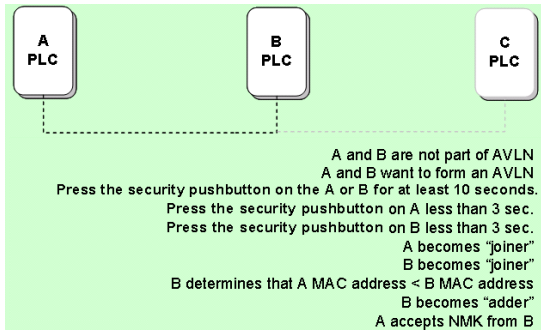
Step 1 Press the **Security** button on the A or B for at least 10 seconds. The device will reset and restart with a random NMK.

Step 2 Press the **Security** button on the first device A for less than 3 seconds.

Step 3 Press the **Security** button on the second device B for less than 3 seconds. Press the button on B within 1 minute.

Step 4 Wait for connection to complete.

The Power LED on both devices will flash evenly at 1-second intervals until the operation succeeds or fails. It will illuminate steadily on successful completion. If an error occurs, the Power LED on the 'adder' will flash unevenly until the pushbutton on the 'adder' is pressed again or the 'joiner' is reset by holding the pushbuttons down for more than 10 seconds.


A
PLC
B
PLC
C
PLC
A and B are not part of AVLN
A and B want to form an AVLN
Press the security pushbutton on the A or B for at least 10 seconds.
Press the security pushbutton on A less than 3 sec.
Press the security pushbutton on B less than 3 sec.
A becomes "joiner"
B becomes "joiner"
B determines that A MAC address < B MAC address
B becomes "adder"
A accepts NMK from B

5.2 Joining a Network

In a scenario where a new device (the joiner) attempts to join an existing network, any devices on the network can become the 'adder'.

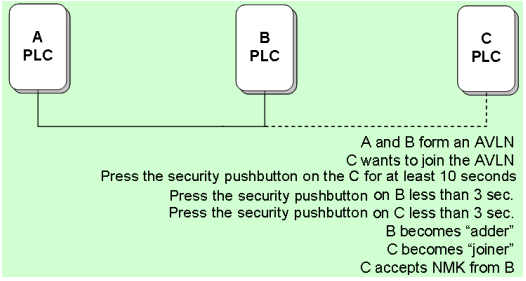
Step 1 Press the **Security** button on the 'joiner' for at least 10 seconds. The device will reset and restart with a random NMK.

Step 2 Press the **Security** button on the 'joiner' for at least 3 seconds.

Step 3 Press the **Security** button on any network device for less than 3 seconds, making it the 'adder'. Please press the **Security** button within 1 minute.

Step 4 Wait for connection to complete.

The Power LED on both devices will flash at 1-second intervals until the process succeeds or fails. It will illuminate steadily on success. If an error occurs, the Power LED on the 'adder' will flash unevenly until the Security button on the 'adder' is pressed again or the 'joiner' is reset by pressing the Security button for more than 10 seconds.


A
PLC
B
PLC
C
PLC
A and B form an AVLN
C wants to join the AVLN
Press the security pushbutton on the C for at least 10 seconds
Press the security pushbutton on B less than 3 sec.
Press the security pushbutton on C less than 3 sec.
B becomes "adder"
C becomes "joiner"
C accepts NMK from B

5.3 Leaving a Network

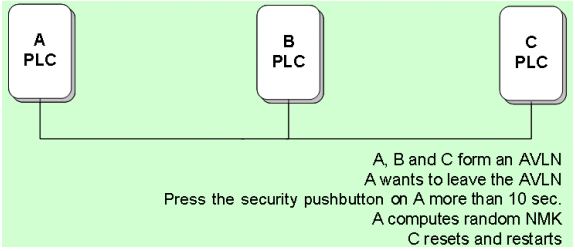
A network exists. The user wants to remove one device, the 'leaver', from that network, for whatever reason. He may want to remove the device from service altogether or have it join another logical network.

Step 1 Press the **Security** button on the 'leaver' for at least 10 seconds. The device will reset and restart with a random NMK.

Step 2 Wait for reset to complete.

The Power LED on the 'leaver' will momentarily extinguish during reset, flash during restart then illuminate steadily. No errors can occur.

Once the process completes, the user may disconnect the device from the medium or join it to another logical network on the same medium.


A
PLC
B
PLC
C
PLC
A, B and C form an AVLN
A wants to leave the AVLN
Press the security pushbutton on A more than 10 sec.
A computes random NMK
C resets and restarts

6 Parameter and Specification

PLC Module SPEC	
Chipset	Intellon INT6400/INT1400
SDRAM:	64 Mbits
Firmware	Support North America/Europe/APAC/Japan
Protocol	HomePlug AV IEEE 802.3 10/100 Ethernet (100Mbps) IEEE 802.3u Fast Ethernet Co-exists with existing HomePlug 1.0
PLC Rate	200Mbit/s
Data Rate - TCP/UDP	65Mbps TCP, 90Mbps UDP
Modulation Band	2-30MHz
Modulation Schemes	Supports 1024/256/64/16/8-QAM, QPSK,BPSK and ROBO
Encryption	128-bit AES
QoS	Support contention-free access, four-level priority based contention access, and multi segment bursting Support VLAN Priority Support ToS and CoS Packet Classifier
Work Mode	TDMA and priority based CSMA/CA
Multicast Support	Supports IGMP managed multicast sessions
WiFi Module SPEC	
Chipset	Atheros AR9331
Serial Flash	64 Mbits
DDR SDRAM:	256 Mbits
Protocol	IEEE 802.11b/g/n IEEE 802.3/3x/3u
Wireless Frequency Range	2.4GHz to 2.484GHz
Channel	1~13
Wireless Signal	11b: 11/5.5/2/1 Mbps

Rates With Automatic Fallback	11g: 54/48/36/24/18/12/9/6 Mbps 11n: 150Mbps in 40MHz mode 72Mbps in 20MHz mode
Transmit Output Power	11n: 13-20dBm 11g: 14-21dBm 11b: 16-22dBm
Receiver Sensitivity	11n: 150Mbps/-69dbM 11g: 54Mbps/-75dBm 11b: 11Mbps/-88dBM
Work mode	1Tx/1Rx
multi-BSSID	Up to 8 BSSIDs
Security	WPA,WPA2,64/128/152-bit,WEP,802.1X,WPA/WPA2-Enterprise SSID hide, MAC Address Access Control List
System SPEC	
System Support	Windows 98SE, 2000, ME, XP 32/64 bit and Vista 32/64bit
LED's	Power: Power on and off PLC: double color, indicator PLC Link and Activity WLAN: indicator Wireless Link and Activity WPS: indicator the status of WPS Authenticator. LAN: indicator the Ethernet Link and Activity
Power Socket	Support British, Euro, Japan, US and China power connector
Ethernet Interface	2 x RJ45 for 10/100 Ethernet (Auto MDI/MDI-X)
Antenna interface	R/SMA x 1
Push Button	Reset: reset system or restore default setup NMK: use to synchronized network password in PLC WPS: use to authenticated for wireless provide service
Software update	Support software update from WEB
Consumption	6 W (Typed)
Environment Requirement	
Operating Temperature	0 ºC to 40 ºC
Storage Temperature	-10 ºC to 70 ºC

Operating Humidity	10% to 85% Non-condensing
Storage Humidity	5% to 90% Non-Condensing
Input Rating	100-240 VAC, 50/60Hz
EMC and Safety	
Regulatory Compliance	FCC Part 15 Class B, CE
Safety Regulations	UL
Green Standard	RoHS
Physical Feature	
Physical Characteristics	L×W×H: 105mm×61mm×46mm
Weight	160g